FACT SHEET

U.S. Army Cyber Command and Second Army
The Nation's Army in Cyberspace
www.arcyber.army.mil

THE FACTS: CYBERSECURITY 101

How can you help keep Army networks safe?

The cyber threat facing the Army is pervasive and increasingly sophisticated. Cyber attacks constantly threaten Army network, information and personnel. Working together, we all play an essential role in keeping our networks, information and personnel safe from harm.

You Need To Know:	**What is it?**	**What should I do?**
Social Engineering	The act of manipulating people into providing sensitive information or performing a desired action. Social engineering can lead to loss of confidential information, systems intrusions and identity theft.	Be suspicious of unsolicited phone calls, emails or individuals asking about organizational or personal information. When submitting personal information, ensure the website is legitimate and starts with HTTPS.
Email Phishing & Spear Phishing	Email-based attacks where the attacker attempts to fool you into taking an action such as clicking a link, opening an attachment by pretending to be a legitimate business or someone you know.	Delete emails you think are a phishing attack. Be suspicious of attachments and links, and only open those you were expecting. Limit the information you post about yourself online.
Fraudulent Websites	Websites that appear legitimate by copying the look of other, well-known sites. These fake websites prey on people who are looking for the lowest price possible by searching the web for products they'd like to buy, and then add words such as "cheapest" or "lowest price." In return, the search engine will present many, even hundreds of websites selling the item, to include the fake sites.	Be wary of unknown stores offering prices dramatically cheaper than anyone else. Look for missing sales or contact information, or different website and email domain names. Shop at trusted online stores that have an established reputation. Monitor your credit card statements to identify suspicious charges.
Theft, Loss or Negligent Disclosure of Information	Loss of control over sensitive and protected data happens when attackers gain unauthorized access to information or when authorized users negligently transfer classified information to a network or computing device with a lower classification.	Always encrypt sensitive information. Do not store or process classified information on any system not approved for classified processing. Review classification levels including hidden data – e.g. notes on PowerPoint slides, images, and recoverable traces of deleted data.
Malware	Software used to perform malicious actions on computing devices, including tablets and smartphones. Attackers' goals can include stealing confidential data, collecting passwords, sending spam emails, or identity theft.	Keep your software up-to-date by enabling automatic updates, install trusted anti-virus software from well-known vendors and be alert for anyone attempting to fool or trick you into infecting your own computer.

ABOUT US: Army Cyber Command and Second Army directs and conducts cyberspace and information operations as authorized or directed, to ensure freedom of action in and through cyberspace, and to deny the same to our adversaries